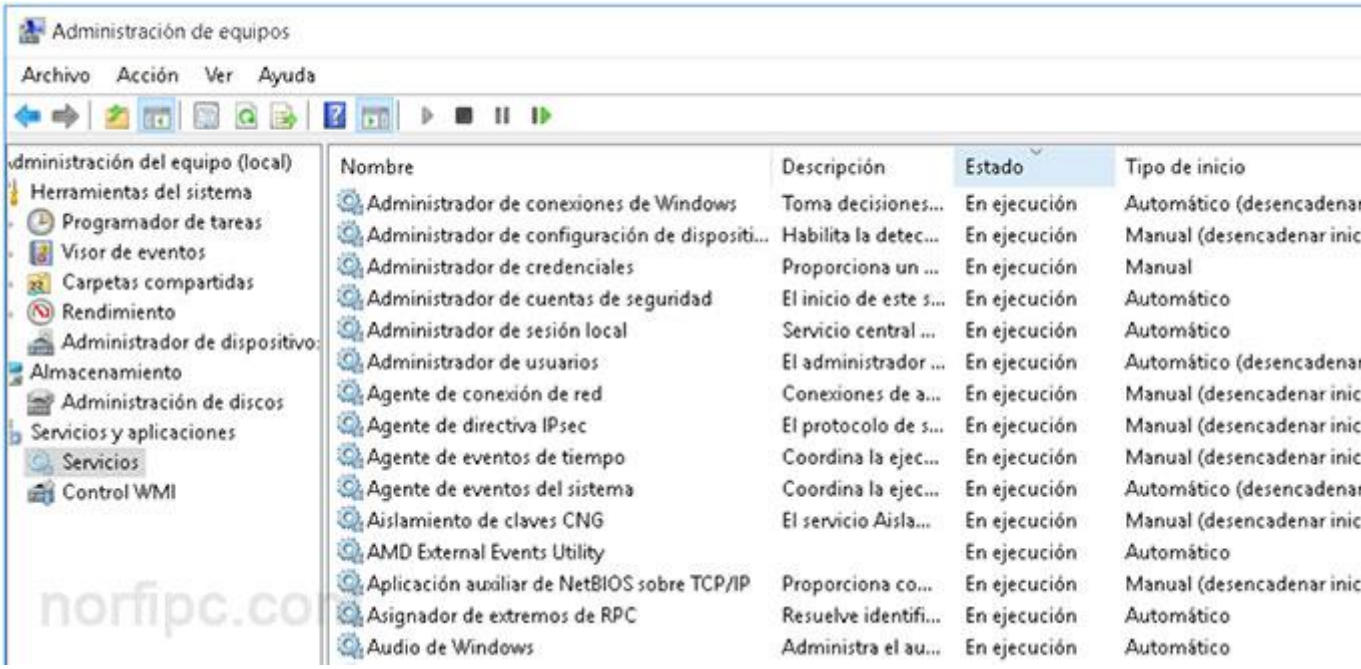
Servicios innecesarios en Windows 10 que podemos detener o desactivar

Lista de servicios que se pueden detener, cambiar su estado a manual o deshabilitar, para mejorar el rendimiento y la rapidez, sin desestabilizar ni afectar funcionalidades del sistema operativo.

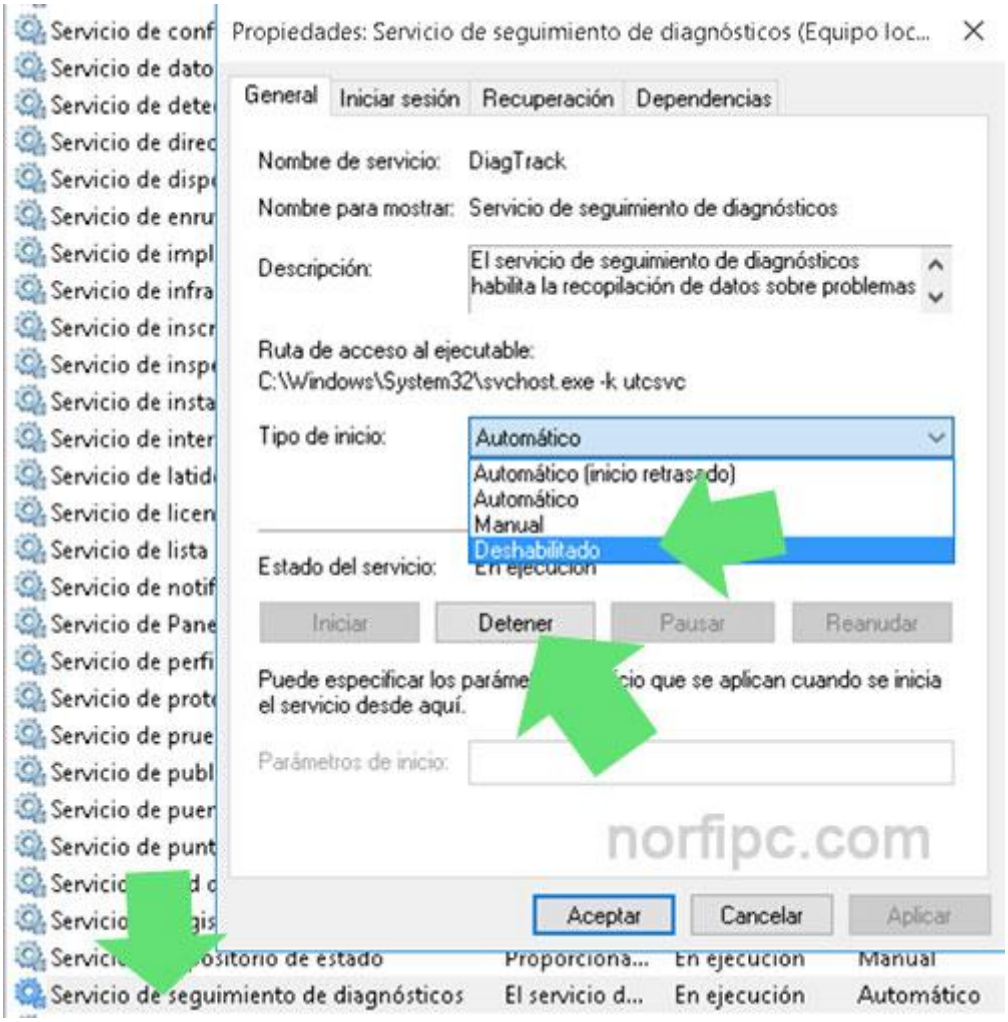
Como en otros artículos dedicados a versiones anteriores de Windows, en este compartimos una lista de los servicios predeterminados del sistema que se pueden deshabilitar o detener y poner en estado Manual, sin peligro alguno.
De esta forma ganamos en rendimiento.
Aunque el título de esta página usa el tradicional termino de "servicios innecesarios", debemos de comprender que todos los servicios son necesarios, pero no para la gran mayoría.
Muchos de ellos inician funcionalidades que a gran parte de nosotros no nos interesan.
Esta lista que compartimos es genérica, cada persona debe analizar si algunos de los servicios que indicamos se relacionan con funciones necesarias para ellos.
Este método beneficia a muchas personas, principalmente aficionados que poseen equipos con pocos recursos de hardware, personas que usan conexiones de internet lentas o costosas y a todo aquel que desee mejorar el rendimiento del sistema operativo.

Como configurar y administrar los servicios en Windows 10

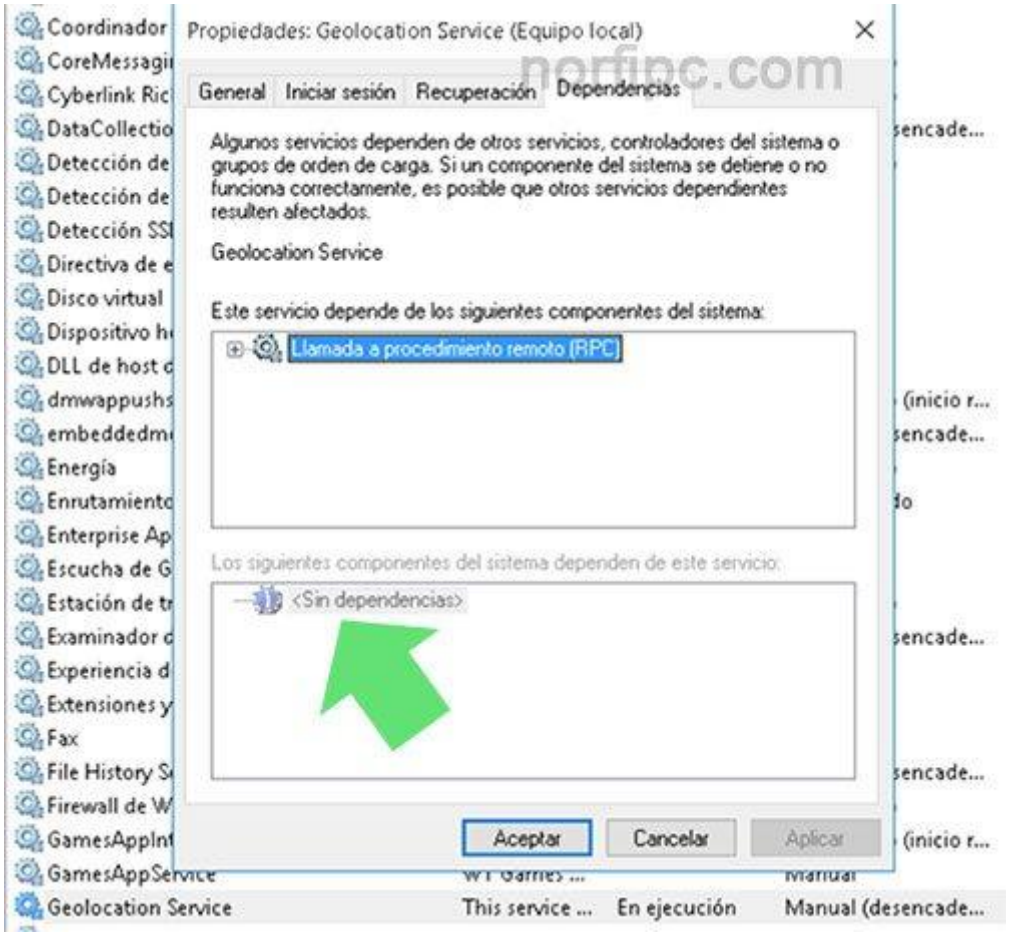
Todos los servicios se administran mediante el panel Servicios.
Para abrirlo haz lo siguiente:
- Da un clic derecho con el ratón en el icono de Este equipo (Mi Pc) y en el menú selecciona Administrar.
- En la ventana Administración de equipos selecciona Servicios.
- Para más comodidad selecciona la pestaña "Estándar" en la parte inferior de la ventana.



Los servicios están ordenados por su nombre, aunque podemos dar un clic encima de las columnas Estado o Tipo de inicio, para listarlos por estos parámetros.
Hay cuatro tipos de inicio:
— Automático. Indica que el servicio lo inicia el sistema u otro servicio de forma automática.
— Automático (Inicio retrasado). Se inicia después de que Windows se haya iniciado completamente.
— Manual. El servicio se inicia por una aplicación o función que inicie el usuario.
— Manual (desencadenar inicio). Es iniciado si no hay demasiados servicios en ejecución.
— Deshabilitado. Servicio que ha sido deshabilitado por el usuario y no se puede iniciar.
Al dar clic encima de uno de los servicios en la lista, se abre el panel de Propiedades.
En su pestaña General podemos Iniciar, Detener, Pausar o Reanudar o iniciar el servicio seleccionado.
Además definir el Tipo de inicio.



En la pestaña Dependencias del mismo panel de Propiedades, podemos conocer si el servicio que deseamos administrar depende de algún componente del sistema o si (más importante aún) algún componente del sistema depende de este servicio para iniciarse.



Lista de servicios que se pueden Detener o Desactivar en Windows 10

En Windows 10 Microsoft introduce más de 50 nuevos servicios y elimina algunos usados en sistemas operativos anteriores.
La siguiente lista corresponde a servicios que se pueden Detener, establecer en estado Manual por si fueran necesarios en alguna tarea específica o Deshabilitar completamente.
- **Administrador de mapas descargados** (MapsBroker). Pueden Deshabilitarlo los que no usen la aplicación Mapas.
- **dmwappushservice** (Servicio de enrutamiento de mensajes de inserción WAP). Deshabilitar para desactivar la Telemetría y recolección de datos por Microsoft.
- **GamesAppIntegrationService**. Pueden detenerlo y deshabilitarlo los que no estén interesados en juegos.
- **IP Helper** (Proporciona compatibilidad con la nueva tecnología IPv6). Pueden detenerlo y establecerlo en manual, los que su conexión a internet no soporta Ipv6.
- **Cola de impresión** (Spooler). Pueden detenerlo y ponerlo en estado Manual los que no usen una impresora.
- **Geolocation Service** (lfsvc). Pueden detenerlo y deshabilitarlo los que no usen servicios de geolocalización y los que desean mantener su privacidad a salvo.
- **Registro remoto** (Permite modificar de forma remota desde otro equipo la configuración del Registro de Windows). Se puede deshabilitar por propósitos de

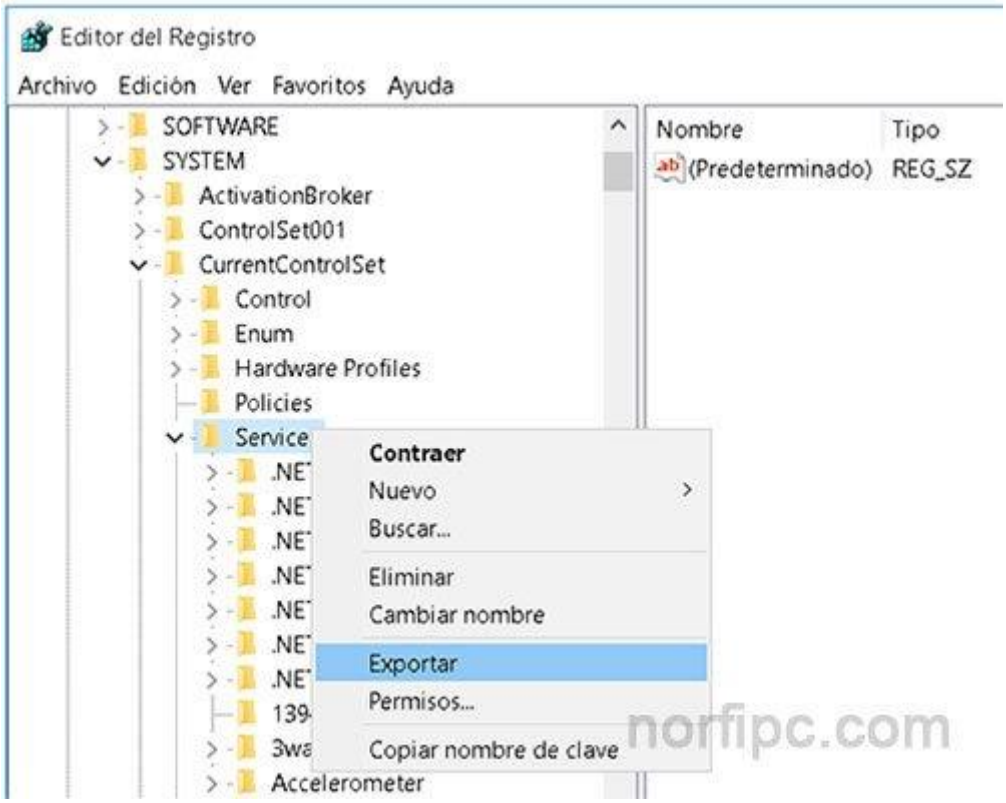
seguridad.
- **Aplicación auxiliar de NetBIOS sobre TCP/IP** (lmhosts). Pueden detenerlo y deshabitarlo los que no usen su equipo en una red local.
- **Security Center** (Centro de seguridad). Monitorea constantemente el sistema, chequea diversos parámetros del antivirus, cortafuegos, Windows Update, control de usuarios y muestra notificaciones llamando a la acción.
Lee mas información
- **Servicio Asistente para la compatibilidad de programas**. Se puede detener y establecer como manual.
- **Servicio de seguimiento de diagnósticos**. Se puede detener y deshabilitar para desactivar la Telemetría y recolección de datos por Microsoft.
- **Servicio de Panel de escritura a mano y teclado táctil**. Pueden detenerlo y deshabilitarlo los que no posean un monitor táctil.
- **Servicio de Windows Defender**. Pueden deshabilitarlo los que traten de usar un programa antivirus/antimalware adicional en el equipo y esto cause algún conflicto.
- **Servicio Informe de errores de Windows** (WerSvc). Pueden Deshabilitar este servicio los que no les interese ni generar ni enviar informes a Microsoft sobre errores en programas o el sistema. De forma predeterminada está en estado manual y se inicia ante cualquier error.
- **Windows Update** (Actualizaciones de Windows). Pueden detenerlo, los que experimenten conflictos por el excesivo consumo de internet del sistema en conexiones lentas y activarlo regularmente para comprobar la existencia de actualizaciones desde Microsoft y descargarlas.
Lee más información: Deshabilitar temporalmente Windows Update en Windows 10
De forma adicional a los servicios anteriores, se pueden detener y establecer como Manual muchos otros que no son de Windows y son instalados por programas del fabricante del equipo.
Abundan especialmente en Laptops para asistencia técnica, información y promoción de nuevos productos.
Generalmente su nombre comienza con el del fabricante (HP, Intel, Cyberlink, Realtek, etc.)
Despues de configurar los servicios necesarios, solo resta cerrar el panel de Servicios y reiniciar Windows.
Inmediatamente nos percataremos de la mejoría en el rendimiento.

Servicios bloqueados en Windows 10

En Windows 10 varios servicios de funcionalidades del sistema están bloqueados y no se puede cambiar su estado.
En esos casos hay que acudir necesariamente al Editor de directivas o al Registro de Windows.
Lee como hacerlo en un caso práctico: Como detener o deshabilitar Windows Defender en Windows 10

Como guardar la configuración de los servicios

Los que deseen guardar un archivo con la configuración predeterminada de los servicios y posteriormente la modificada, pueden hacerlo exportando la siguiente clave del Registro como un archivo REG:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services



Lee más información detallada: ¿Cómo guardar la configuración predeterminada de los servicios en Windows?

Notificaciones de activar el Centro de seguridad

Después de desactivar el servicio Security Center (Centro de seguridad), comenzaremos a recibir molestas notificaciones de Windows en cada inicio, indicando activar el Centro de seguridad.
Para eliminarlas haz lo siguiente:
1- En el panel de Configuración abre Sistema -> Notificaciones y acciones.
2- Desactiva: "Mostrarme sugerencias de Windows" y "Mostrarme notificaciones de las aplicaciones".
3- Más abajo en Mostrar notificaciones de estas aplicaciones, desactiva "Seguridad y mantenimiento" (en algunas versiones de Windows no aparece esta opción).

Como evitar en Windows 10 el consumo excesivo de internet

Como optimizar la conexión de internet, conocer las aplicaciones que consumen mucho ancho de banda y desactivarlas. Como configurar las actualizaciones o deshabilitar Windows Update. Medidas para mejorar el rendimiento de la navegación.

Después de instalar y de comenzar a usar Windows 10, con una conexión de internet de 1 MB, nos dimos cuenta de que casi es imposible trabajar, porque el sistema consumía más del 50% del ancho de banda de la conexión.
Windows 10 es un modernos y sofisticado sistema operativo, pero que requiere equipos con recursos de hardware y una conexión de internet con un enorme ancho de banda.
En este artículo de utilidad para los que poseen una conexión de internet limitada y costosa, comparto como solucione la situación.

Causas del consumo de ancho de banda en Windows 10

Las causas del excesivo consumo del ancho de banda en Windows 10 son varias, incluyendo aplicaciones que se inician automáticamente y usan la conexión, pero principalmente la función de Windows Update.
Windows Update es la herramienta mediante la cual Microsoft entrega e instala las actualizaciones del sistema operativo, que incluyen nuevas funciones y parches a las existentes.
También actualiza las aplicaciones instaladas de forma predeterminada.

Como optimizar nuestra conexión de internet en Windows 10

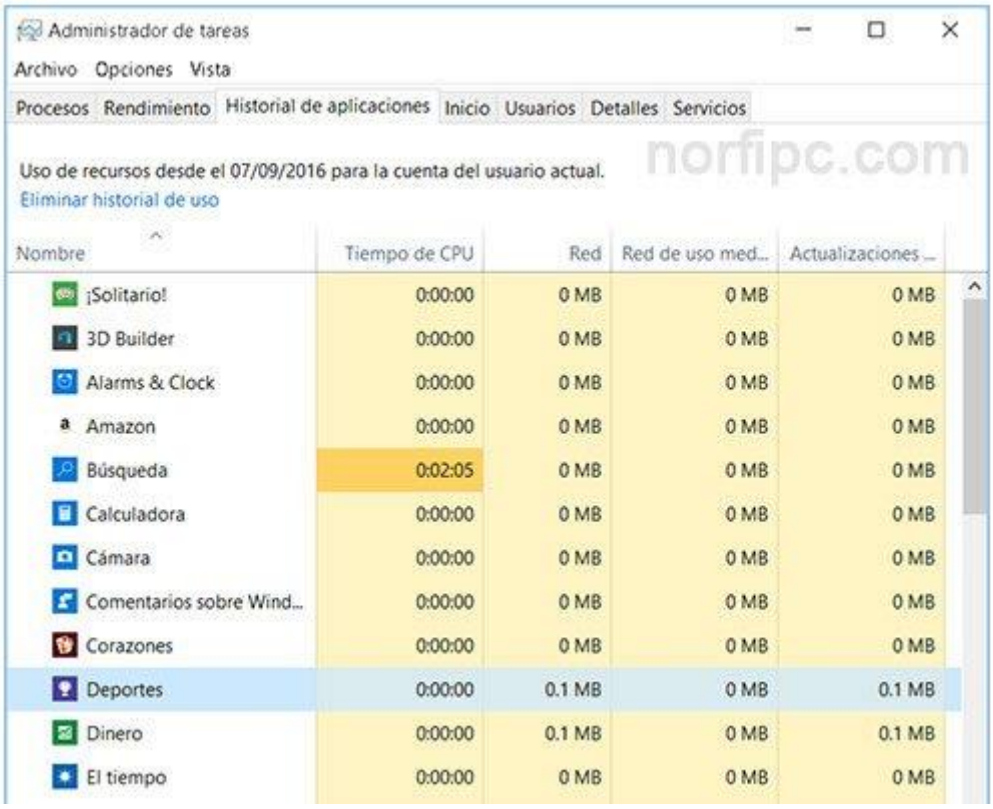
Para optimizar nuestra conexión de internet en Windows 10, debemos seguir los siguientes pasos:
1- Conocer que aplicaciones innecesarias consumen internet.
2- Desactivarlas o deshabilitarlas y si es posible sustituirlas por las del fabricante e instalarlas manualmente.
3- Limitar el consumo de Windows Update, aunque es opcional desactivar la función temporalmente y activarla regularmente para conocer las actualizaciones disponibles.

Conocer que aplicaciones innecesarias consumen internet

De forma predeterminada varias aplicaciones se inician con el sistema, dependiendo del fabricante, en los casos de equipos con Windows preinstalado.
Se pueden conocer cuáles son y desactivarlas en al Administrador de Tareas.
Haz lo siguiente:
1- Da un clic derecho con el ratón en la barra de tareas y en el menú escoge "Administrador de Tareas".
2- Abre el panel "Inicio".
3- Selecciona las aplicaciones habilitadas que no necesitas u deshabilítalas.

En mi caso lo hice con las aplicaciones OneDrive y DropBox que no empleo y consumen bastantes recursos de la red.
4- A continuación abrimos la pestaña "Historial de aplicaciones".
En ella veremos una lista de todas las aplicaciones preinstaladas por Windows, con información de cada una sobre: el tiempo de uso, actividad de red y consumo en

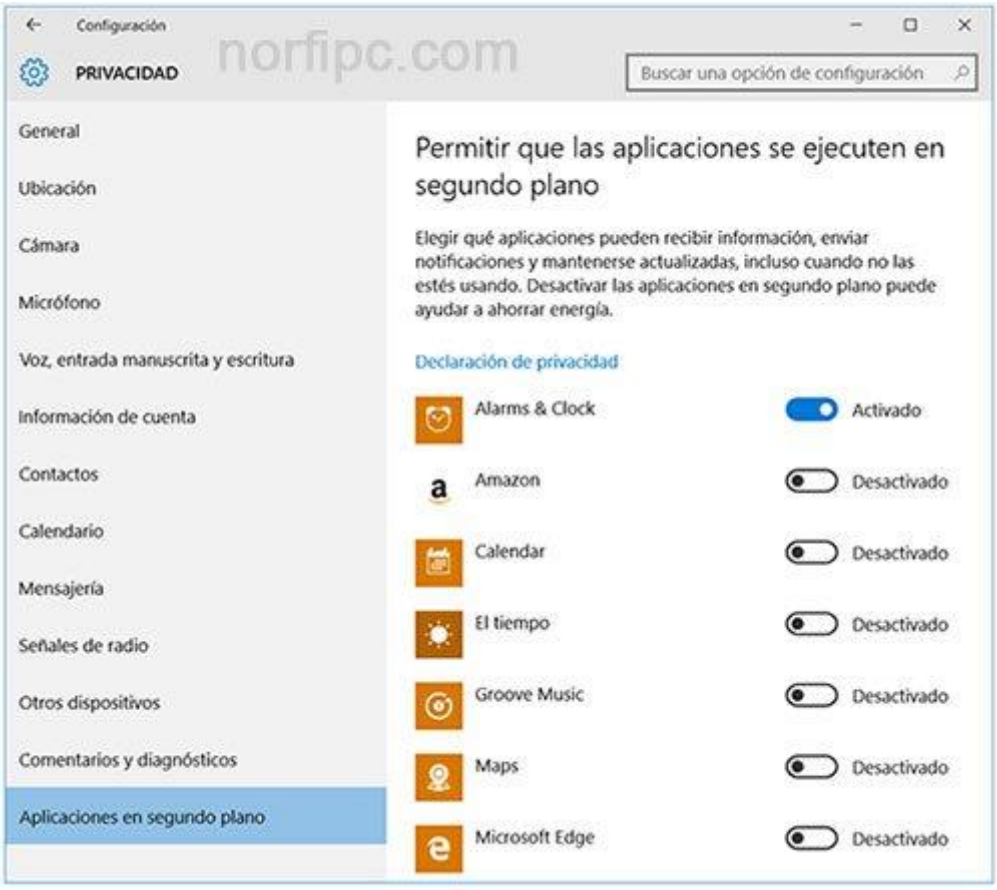
actualizaciones.



De los valores de consumo de la red y de la utilidad de cada aplicación para nosotros, decidiremos si seguiremos empleándolas o las desinstalamos.
La gran mayoría de ellas se pueden desinstalar totalmente, como explicamos en otro artículo: Como desinstalar aplicaciones predeterminadas en Windows 10

Deshabilitar aplicaciones en segundo plano en Windows 10

Windows mantiene una serie de aplicaciones, de las instaladas de forma predeterminada, funcionando en segundo plano y conectándose a internet, aunque no las utilicemos.
Para desactivar este comportamiento, haz lo siguiente:
1- Abre el panel de Configuración.
2- Abre Privacidad -> Aplicaciones en segundo plano.
3-Desactiva las que no sean de tu interés (la lista es mucho superior que las que se muestran en la imagen).



Configurar o desactivar Windows Update en Windows 10

En Windows 8 y versiones anteriores era posible configurar Windows Update, para que dejara de entregar actualizaciones, en Windows 10 no es posible.
La causa es que Microsoft emplea esta función para controlar relativamente el sistema. Por ejemplo obligar al usuario a actualizar, restringir o bloquear funciones, etc.
No obstante siempre es posible atenuar estas afectaciones de varios modos o deshabilitar temporalmente Windows Update.

Configurar las actualizaciones en Windows 10

Los que deseen optimizar la forma en que Microsoft entrega las actualizaciones, pueden hacer lo siguiente:
1- Usa las teclas Windows + I para abrir el panel de Configuración.
Selecciona Actualización y seguridad y después Windows Update -> Opciones avanzadas.
2- En Elige como quieres instalar las actualizaciones, escoge en el menú "Notificar para programar reinicio".

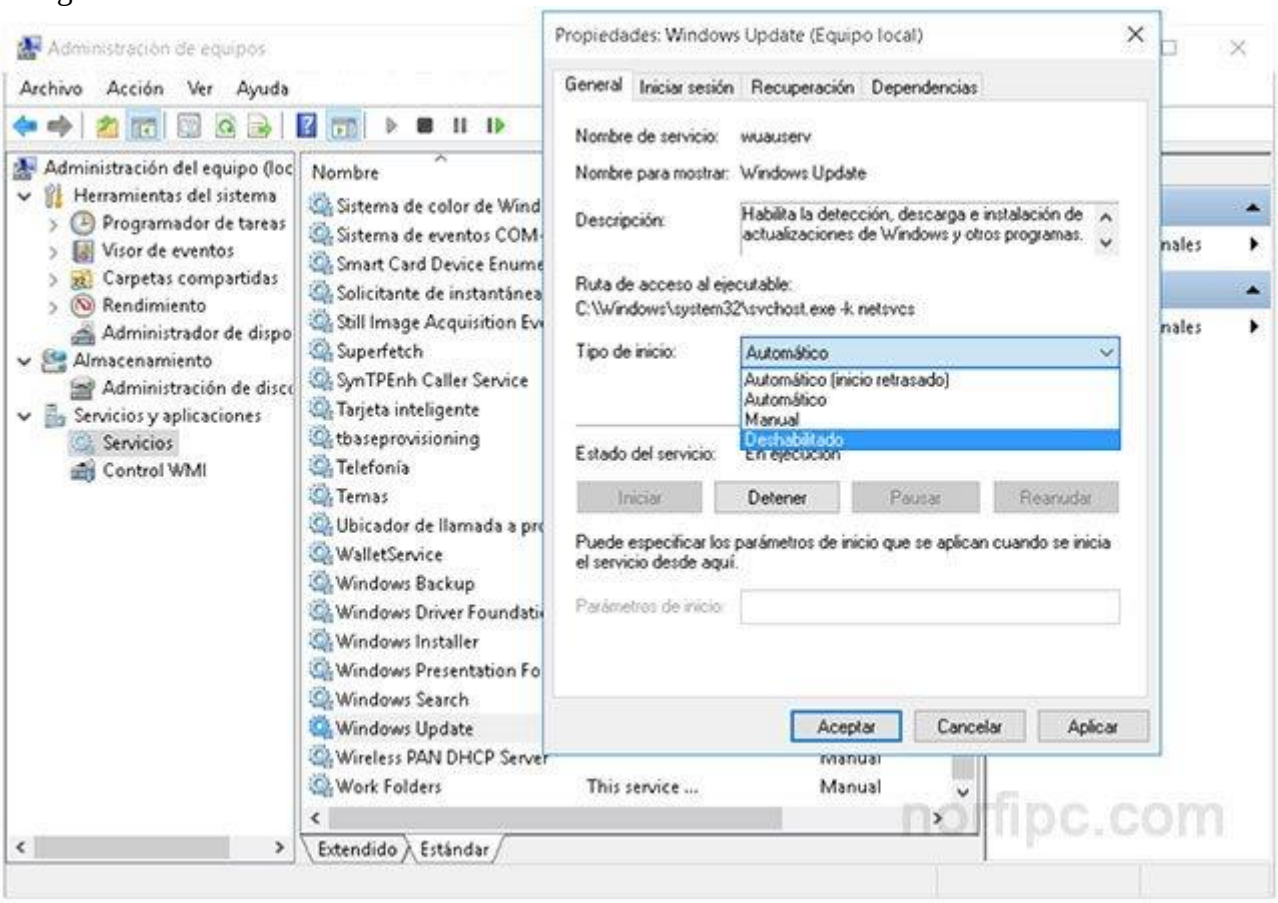
Esto no impedirá que Windows Update este revisando constantemente en busca de actualizaciones, solo aplazará la descarga e instalación de las mismas.
3- A continuación desciende hasta Elegir como se entregan las actualizaciones.
4- Desactiva el botón de descargar actualizaciones desde otros equipos.

Esto impedirá que tu equipo no forme parte de una red P2P, para recibir, pero también para enviar actualizaciones a otras computadoras, consumiendo tu ancho de banda para servirle de apoyo a Microsoft.

Deshabilitar temporalmente Windows Update

Los que deseen deshabilitar temporalmente Windows Update, pueden deshabilitar el servicio, aunque siempre es posible en cualquier momento volver a activarlo.
Para eso haz lo siguiente:
1- Da un clic derecho en el icono de Este equipo (Mi PC) y en el menú escoge "Administrar".

2- Abre Servicios y aplicaciones -> Servicios.
3- Desciende hasta el servicio Windows Update da dos clics.
4- En el panel presiona el botón "Detener" y después que se detenga en Tipo de servicio escoge "Deshabilitado".



5- Guarda los cambios.

Obtención de contraseña de usuario en Windows 10 décimo aniversario

Dejar un comentario / Ataques, Herramientas, Mimikatz, Windows / Por Alejandro Fernández / viernes, 14 diciembre, 2018

En esta entrada aprenderemos a recuperar la contraseña de un usuario en un Windows 10 con la actualización del décimo aniversario.

En primer lugar, vamos a definir los ficheros y herramientas que vamos a emplear para llevar a cabo este ejercicio:

- **SAM:** son las siglas de Security Account Manager, este fichero se encarga de almacenar credenciales de los usuarios del sistema en Windows. Dentro de la SAM las contraseñas se almacenan en formato hash.

- **SYSKEY:** este fichero se creó, a partir de Windows 2000, para proteger la SAM frente a ataques offline. Si se habilita el uso de este fichero, las hashes almacenadas en la SAM se cifrarán con una clave conocida como syskey.
- **Mimikatz:** es una herramienta desarrollada en C para realizar diferentes pruebas de seguridad en sistemas Windows. Se suele usar habitualmente para obtener contraseñas y hashes de contraseñas, aunque también permite realizar ataques de tipo Pass-The-Hash.
- **Pwdump:** esta herramienta nos permite volcar el contenido de la SAM.
- **Hashcat:** poderosa herramienta para la recuperación de contraseñas. Nos permite diferentes tipos de ataques sobre las contraseñas y admite multitud de tipos de hash.

El escenario que tenemos el siguiente, un usuario ha olvidado la contraseña de acceso de su portátil, en el cual tiene Windows 10 como sistema operativo.

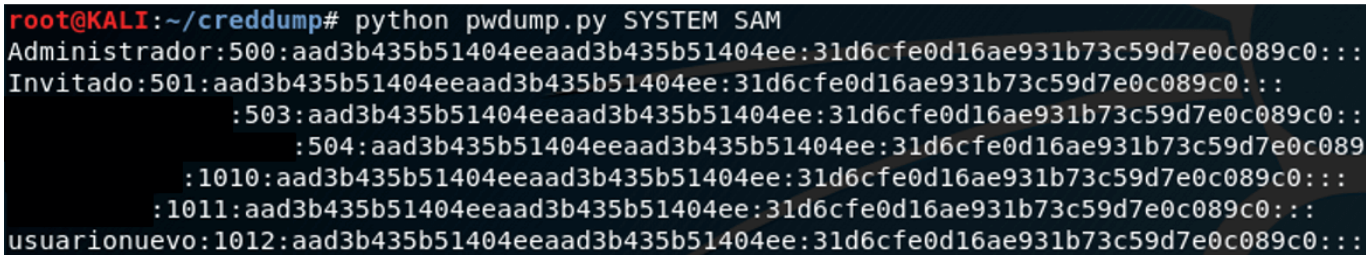
Como no podemos iniciar sesión en el sistema, arrancaremos desde un LiveCD con Kali Linux, ya que el primer paso será la adquisición de los ficheros **SAM** y **SYSKEY**.

Una vez arrancado el sistema operativo debemos ir a la ruta donde se almacenan estos ficheros, dicha ruta es la siguiente:

```
C:\Windows\System32
```

Copiaremos los ficheros a unidad extraíble y nos los llevaremos a nuestra máquina para obtener las contraseñas almacenadas.

Si usamos **pwdump** para visualizar el contenido de la **SAM**, observaremos lo siguiente:



El formato que nos muestra **pwdump** se compone de:

Nombre de usuario : ID de usuario : Hash de la contraseña en LM : Hash de la contraseña en NTLM

Como se puede ver en la imagen, todos los usuarios tienen las mismas hashes. Estas hashes son el resultado de una contraseña vacía. Desde la actualización del décimo aniversario de Windows la forma de almacenar las hashes en la **SAM** cambia y es por eso por lo que el programa **pwdump** no consigue identificar correctamente las hashes de los usuarios.

Hash

aad3b435b51404eeaad3b435b51404ee

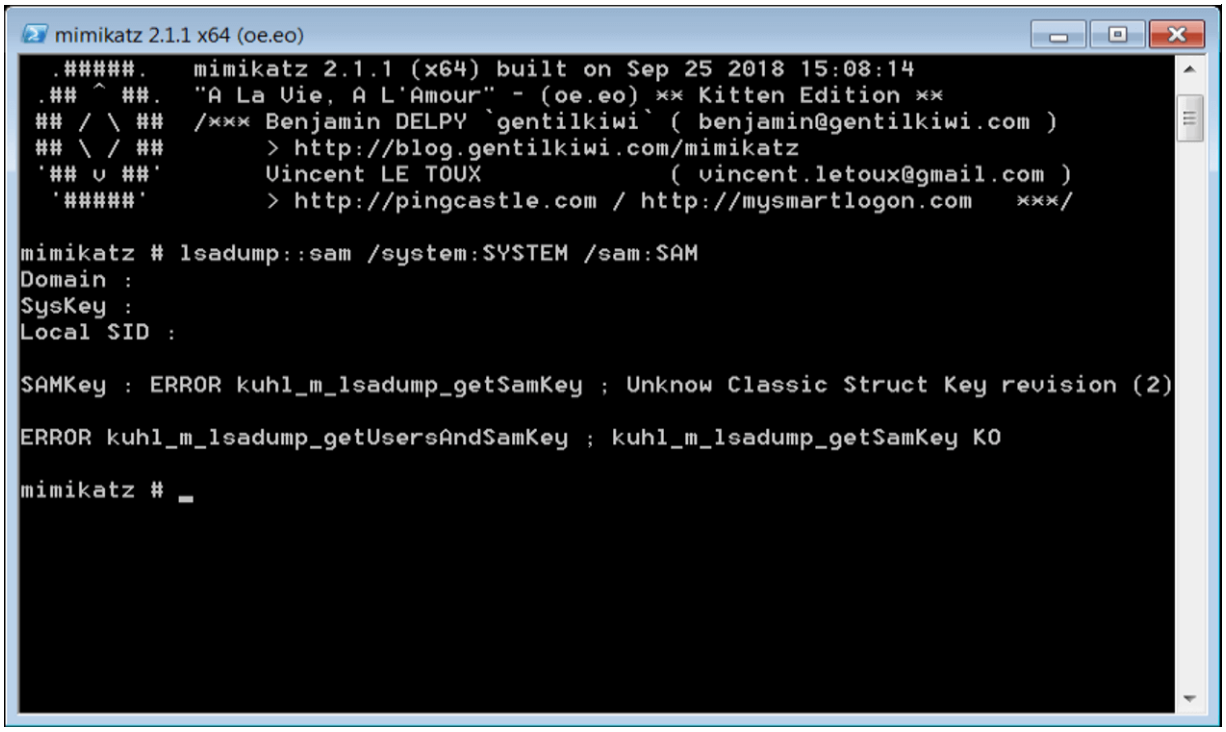
31d6cfe0d16ae931b73c59d7e0c089c0

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Haciendo uso de **mimikatz**, intentaremos obtener las hashes correctas mediante el módulo lsadump, dicho módulo nos permite obtener las hashes de manera «offline», es decir, proporcionando a la herramienta los ficheros **SAM** y **SYSTEM**.

Tras ejecutar dicho módulo para obtener las hashes, obtenemos el siguiente error:

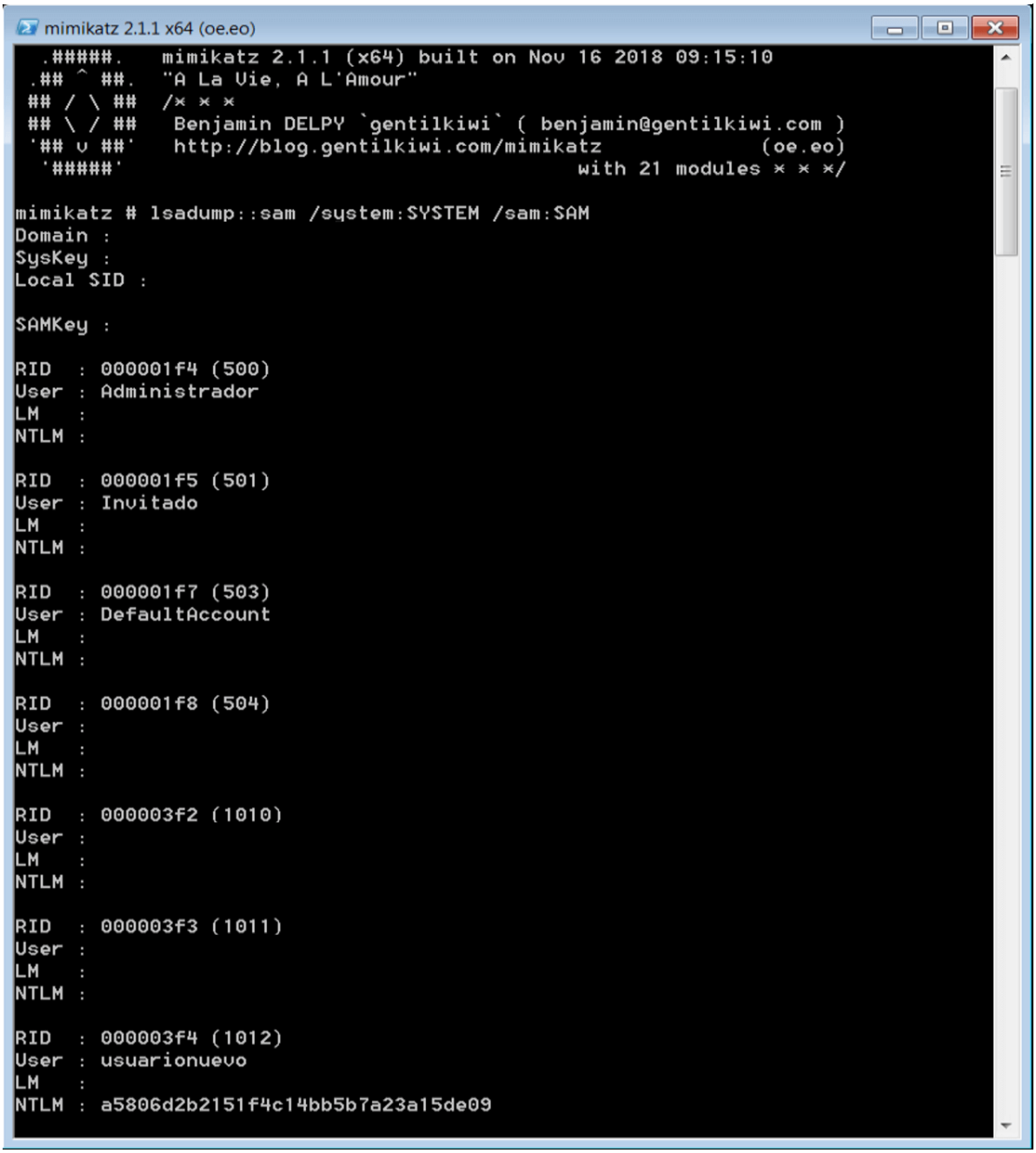
```
SAMKey :  ERROR kuhl_m_lsadump_getSamKey : Unknow Classic Struct Key
revision (2)

ERROR kuhl_m_lsadump_getUsersAndSamKey ; kuhl_m_lsadump_getSamKey KO
```



Buscando información sobre este error, encontramos un **issue** en el repositorio de la herramienta que nos dice cómo debemos solventar el error.

Si comprobamos el código fuente de la última versión de **mimikatz**, veremos que el código no está aún parcheado, por lo que deberemos descargar el código fuente, modificarlo y volver a compilarlo para que así funcione correctamente. Para ello tal y como nos dice el creador de **mimikatz** en su repositorio, deberemos usar **Visual Studio Code**.

Una vez modificado el código y compilada la herramienta, volveremos a ejecutar el módulo lsadump, para obtener correctamente las hashes de los usuarios del sistema.



Una vez obtenida la hash, podremos realizar un ataque de diccionario sobre la misma para obtener la contraseña en texto claro.

Haciendo uso de la herramienta **hashcat** realizaremos el ataque.

```
root@KALI:~# hashcat -m 1000 -a 0 hash.txt dictionary.txt -o out.txt --force
hashcat (v4.1.0) starting...
```

Los parámetros usados para la realización del ataque son los siguientes:

- **-m 1000:** para indicar el tipo de hash NTLM.
- **-a 0:** para seleccionar el tipo de ataque, en este caso por diccionario.
- **hash.txt:** fichero que contiene la hash a descifrar.
- **dictionary.txt:** diccionario empleado para el ataque.
- **-o out.txt:** fichero que guarda el resultado del ataque.
- **–force:** para ignorar warnings.

Una vez finalizada la ejecución de la herramienta, en el fichero out.txt podremos obtener la contraseña correspondiente a la hash «atacada», en texto claro.

Para facilitar a todos los que se encuentren con este problema, he creado un repositorio en mi Github con el código fuente, modificado para solventar el error, de la herramienta y el ejecutable correspondiente. Para acceder al repositorio pulsa **aquí**.

Recientemente el creador de la herramienta ha subido una nueva release (10 de Diciembre) a su repositorio que aún no solventa este error.